Knowledge Brings Fear

At some point in time, you recognize that knowing more does not necessarily make you more happy. This weblog is about both: knowledge and happiness.

Welcome to the world of tomorrow

We lost the war. Welcome to the world of tomorrow.

by: Frank Rieger, frank@ccc.de, 20. December 2005

Losing a war is never a pretty situation. So it is no wonder that most people do not like to acknowledge that we have lost. We had a reasonable chance to tame the wild beast of universal surveillance technology, approximately until september 10th, 2001. One day later, we had lost. All the hopes we had, to keep the big corporations and "security forces" at bay and develop interesting alternative concepts in the virtual world, evaporated with the smoke clouds of the World Trade Center.

Just right before, everything looked not too bad. We had survived Y2K with barely a scratch. The world's outlook was mildly optimistic after all. The "New Economy" bubble gave most of us fun things to do and the fleeting hope of plenty of cash not so far down the road. We had won the Clipper-Chip battle, and crypto-regulation as we knew it was a thing of the past. The waves of technology development seemed to work in favor of freedom, most of the time. The future looked like a yellow brick road to a nirvana of endless bandwith, the rule of ideas over matter and dissolving nation states. The big corporations were at our mercy because we knew what the future would look like and we had the technology to built it. Those were the days. Remember them for your grandchildren's bedtime stories. They will never come back again.

We are now deep inside the other kind of future, the future that we speculated about as a worst case scenario, back then. This is the ugly future, the one we never wanted, the one that we fought to prevent. We failed. Probably it was not even our fault. But we are forced to live in it now.

Democracy is already over

By its very nature the western democracies have become a playground for lobbyists, industry interests and conspiracies that have absolutely no interest in real democracy. The "democracy show" must go on nonetheless. Conveniently, the show consumes the energy of those that might otherwise become dangerous to the status quo. The show provides the necessary excuse when things go wrong and keeps up the illusion of participation. Also, the system provides organized and regulated battleground rules to find out which interest groups and conspiracies have the upper hand for a while. Most of the time it prevents

open and violent power struggles that could destabilize everything. So it is in the best interest of most players to keep at least certain elements of the current “democracy show” alive. Even for the more evil conspiracies around, the system is useful as it is. Certainly, the features that could provide unpleasant surprises like direct popular votes on key issues are the least likely to survive in the long run.

Of course, those in power want to minimize the influence of random chaotic outbursts of popular will as much as possible. The real decisions in government are not made by ministers or the parliament. The real power of government rests with the undersecretaries and other high-level, non-elected civil servants who stay while the politicians come and go. Especially in the bureaucracies of the intelligence agencies, the ministry of interior, the military, and other key nodes of power the long-term planning and decision-making is not left to the incompetent mediocre political actors that get elected more or less at random. Long term stability is a highly valued thing in power relations. So even if the politicians of states suddenly start to be hostile to each other, their intelligence agencies will often continue to cooperate and trade telecommunication interception results as if nothing has happened.

Let’s try for a minute to look at the world from the perspective of such an 60-year-old bureaucrat that has access to the key data, the privilege to be paid to think ahead, and the task to prepare the policy for the next decades. What he would see, could look like this:â€¨

First,
paid manual labor will be eaten away further by technology, even more rapidly than today. Robotics will evolve far enough to kill a sizeable chunk of the remaining low-end manual jobs. Of course, there will be new jobs, servicing the robots, biotech, designing stuff, working on the nanotech developments etc. But these will be few, compared with today, and require higher education. Globalization continues its merciless course and will also export a lot of jobs of the brain-labor type to India and China, as soon as education levels there permit it.

So the western societies will end up with a large percentage of population, at least a third, but possibly half of those in working age, having no real paid work. There are those whose talents are cheaper to be had elsewhere, those who are more inclined to manual labor. Not only the undereducated but all those who simply cannot find a decent job anymore. This part of the population needs to be pacified, either by Disney or by Dictatorship, most probably by both. The unemployment problem severely affects the ability of states to pay for social benefits. At some point it becomes cheaper to put money into repressive police forces and rule by fear than put the money into pay-outs to the unemployed population and buy the social peace. Criminal activities look more interesting when there is no decent job to be had. Violence is the unavoidable consequence of degrading social standards. Universal surveillance might dampen the consequences for those who remain with some wealth to defend.â€¨

Second,
climate change increases the frequency and devastation of natural disasters, creating large scale emergency situations. Depending on geography, large parts of land may become uninhabitable due to draught, flood, fires or plagues. This creates a multitude of unpleasant effects. A large number of people need to move, crop and animal production shrinks, industrial centers and cities may be damaged to the point where abandoning them is the only sensible choice left. The loss of property like non-usable (or

non-insurable) real estate will be frightening. The resulting internal migratory pressures towards “safe areas” become a significant problem. Properly trained personal, equipment, and supplies to respond to environmental emergencies are needed standby all the time, eating up scarce government resources. The conscript parts of national armed forces may be formed into disaster relief units as they hang around anyway with no real job to do except securing fossil energy sources abroad and helping out the border police.

Third,
immigration pressure from neighboring regions will raise in all western countries. It looks like the climate disaster will strike worst at first in areas like Africa and Latin America and the economy there is unlikely to cope any better than the western countries with globalization and other problems ahead. So the number of people who want to leave from there to somewhere inhabitable at all costs will rise substantially. The western countries need a certain amount of immigration to fill up their demographic holes but the number of people who want to come will be far higher. Managing a controlled immigration process according to the demographic needs is a nasty task where things can only go wrong most of the time. The nearly unavoidable reaction will be a Fortress Europe: serious border controls and fortifications, frequent and omnipresent internal identity checks, fast and merciless deportation of illegal immigrants, biometrics on every possible corner. Technology for border control can be made quite efficient once ethical hurdles have fallen.

Fourth,
at some point in the next decades the energy crisis will strike with full force. Oil will cost a fortune as production capacities can no longer be extended economically to meet the rising demand. Natural gas and coal will last a bit longer, a nuclear renaissance may dampen the worst of the pains. But the core fact remains: a massive change in energy infrastructure is unavoidable. Whether the transition will be harsh, painful and society-wrecking, or just annoying and expensive depends on how soon before peak oil the investments into new energy systems start on a massive scale as oil becomes to expensive to burn. Procrastination is a sure recipe for disaster. The geo-strategic and military race for the remaining large reserves of oil has already begun and will cost vast resources.

Fifth,
we are on the verge of technology developments that may require draconic restrictions and controls to prevent the total disruption of society. Genetic engineering and other biotechnology as well as nanotechnology (and potentially free energy technologies if they exist) will put immense powers into the hands of skilled and knowledgeable individuals. Given the general raise in paranoia, most people (and for sure those in power) will not continue to trust that common sense will prevent the worst. There will be a tendency of controls that keep this kind of technology in the hands of “trustworthy” corporations or state entities. These controls, of course, need to be enforced, surveillance of the usual suspects must be put in place to get advanced knowledge of potential dangers. Science may no longer be a harmless, self-regulating thing but something that needs to be tightly controlled and regulated, at least in the critical areas. The measures needed to contain a potential global pandemic from the Strange Virus of the Year are just a subset of those needed to contain a nanotech or biotech disaster.

Now what follows from this view of the world? What changes to society are required to cope with these

trends from the viewpoint of our 60-year-old power brokering bureaucrat?

Strategically it all points to massive investments into internal security.
Presenting the problem to the population as a mutually exclusive choice between an uncertain dangerous freedom and an assured survival under the securing umbrella of the trustworthy state becomes more easy the further the various crises develop. The more wealthy parts of the population will certainly require protection from illegal immigrants, criminals, terrorists and implicitly also from the anger of less affluent citizens. And since the current system values rich people more then poor ones, the rich must get their protection. The security industry will certainly be of happy helpful assistance, especially where the state can no longer provide enough protection for the taste of the lucky ones.

Traditional democratic values have been eroded to the point where most people don't care anymore. So the loss of rights our ancestors fought for not so long ago is at first happily accepted by a majority that can easily be scared into submission. "Terrorism" is the theme of the day, others will follow. And these "themes" can and will be used to mold the western societies into something that has never been seen before: a democratically legitimated police state, ruled by an unaccountable elite with total surveillance, made efficient and largely unobtrusive by modern technology. With the enemy (immigrants, terrorists, climate catastrophe refugees, criminals, the poor, mad scientists, strange diseases) at the gates, the price that needs to be paid for "security" will look acceptable.

Cooking up the "terrorist threat" by apparently stupid foreign policy and senseless intelligence operations provides a convenient method to get through with the establishment of a democratically legitimized police state. No one cares that car accidents alone kill many more people than terrorists do. The fear of terrorism accelerates the changes in society and provides the means to get the suppression tools required for the coming waves of trouble.

What we call today "anti-terrorism measures" is the long-term planned and conscious preparation of those in power for the kind of world described above.

The Technologies of Oppression

We can imagine most of the surveillance and oppression technology rather well. Blanket CCTV coverage is reality in some cities already. Communication pattern analysis (who talks to whom at what times) is frighteningly effective. Movement pattern recording from cellphones, traffic monitoring systems, and GPS tracking is the next wave that is just beginning. Shopping records (online, credit and rebate cards) are another source of juicy data. The integration of all these data sources into automated behavior pattern analysis currently happens mostly on the dark side.

The key question for establishing an effective surveillance based police state is to keep it low-profile enough that "the ordinary citizen" feels rather protected than threatened, at least until all the pieces are in place to make it permanent. First principle of 21st century police state: All those who "have nothing to hide" should not be bothered unnecessarily. This goal becomes even more complicated as with the increased availability of information on even minor everyday infringements the "moral" pressure to prosecute will rise. Intelligence agencies have always understood that effective work with interception results

requires a thorough selection between cases where it is necessary to do something and those (the majority) where it is best to just be silent and enjoy.

Police forces in general (with a few exceptions) on the other hand have the duty to act upon every crime or minor infringement they get knowledge of. Of course, they have a certain amount of discretion already. With access to all the information outlined above, we will end up with a system of selective enforcement. It is impossible to live in a complex society without violating a rule here and there from time to time, often even without noticing it. If all these violations are documented and available for prosecution, the whole fabric of society changes dramatically. The old sign for totalitarian societies – arbitrary prosecution of political enemies – becomes a reality within the framework of democratic rule-of-law states. As long as the people affected can be made looking like the enemy-"theme" of the day, the system can be used to silence opposition effectively. And at some point the switch to open automated prosecution and policing can be made as any resistance to the system is by definition "terrorism". Development of society comes to a standstill, the rules of the law and order paradise can no longer be violated.

Now disentangling ourselves from the reality tunnel of said 60-year-old bureaucrat, where is hope for freedom, creativity and fun? To be honest, we need to assume that it will take a couple of decades before the pendulum will swing back into the freedom direction, barring a total breakdown of civilization as we know it. Only when the oppression becomes to burdensome and open, there might be a chance to get back to overall progress of mankind earlier. If the powers that be are able to manage the system smoothly and skillfully, we cannot make any prediction as to when the new dark ages will be over.

So what now?

â€¨
Move to the mountains, become a gardener or carpenter, search for happiness in communities of like minded people, in isolation from the rest of the world? The idea has lost its charm for most who ever honestly tried. It may work if you can find eternal happiness in milking cows at five o'clock in the morning. But for the rest of us, the only realistic option is to try to live in, with, and from the world as bad it has become. We need to built our own communities nonetheless, virtual or real ones.

The politics & lobby game

So where to put your energy then? Trying to play the political game, fighting against software patents, surveillance laws, and privacy invasions in parliament and the courts can be the job of a lifetime. It has the advantage that you will win a battle from time to time and can probably slow things down. You may even be able to prevent a gross atrocity here and there. But in the end, the development of technology and the panic level of the general population will chew a lot of your victories for breakfast.

This is not to discount the work and dedication of those of us who fight on this front. But you need to have a lawyers mindset and a very strong frustration tolerance to gain satisfaction from it, and that is not given to everyone. We need the lawyers nonetheless.

Talent and Ethics

Some of us sold their soul, maybe to pay the rent when the bubble bursted and the cool and morally easy jobs became scarce. They sold their head to corporations or the government to built the kind of things we knew perfectly well how to built, that we sometimes discussed as a intellectual game, never intending to make them a reality. Like surveillance infrastructure. Like software to analyze camera images in realtime for movement patterns, faces, license plates. Like data mining to combine vast amounts of information into graphs of relations and behavior. Like interception systems to record and analyze every single phone call, e-mail, click in the web. Means to track every single move of people and things.

Thinking about what can be done with the results of one's work is one thing. Refusing to do the job because it could be to the worse of mankind is something completely different. Especially when there is no other good option to earn a living in a mentally stimulating way around. Most projects by itself were justifiable, of course. It was "not that bad" or "no real risk". Often the excuse was "it is not technical feasible today anyway, it's too much data to store or make sense from". Ten years later it is feasible. For sure.

While it certainly would be better when the surveillance industry would die from lack of talent, the more realistic approach is to keep talking to those of us who sold their head. We need to generate a culture that might be compared with the sale of indulgences in the last dark ages: you may be working on the wrong side of the barricade but we would be willing to trade you private moral absolution in exchange for knowledge. Tell us what is happening there, what the capabilities are, what the plans are, which gross scandals have been hidden. To be honest, there is very little what we know about the capabilities of todays dark-side interception systems after the meanwhile slightly antiquated Echelon system had been discovered. All the new stuff that monitors the internet, the current and future use of database profiling, automated CCTV analysis, behavior pattern discovery and so on is only known in very few cases and vague outlines.

We also need to know how the intelligence agencies work today. It is of highest priority to learn how the "we rather use backdoors than waste time cracking your keys"-methods work in practice on a large scale and what backdoors have been intentionally built into or left inside our systems. Building clean systems will be rather difficult, given the multitude of options to produce a backdoor – ranging from operating system and application software to hardware and CPUs that are to complex to fully audit. Open Source does only help in theory, who has the time to really audit all the source anyway…

Of course, the risk of publishing this kind of knowledge is high, especially for those on the dark side. So we need to build structures that can lessen the risk. We need anonymous submission systems for documents, methods to clean out eventual document fingerprinting (both on paper and electronic). And, of course, we need to develop means to identify the inevitable disinformation that will also be fed through these channels to confuse us.

Building technology to preserve the options for change

We are facing a unprecedented onslaught of surveillance technology. The debate whether this may or may not reduce crime or terrorism is not relevant anymore. The de-facto impact on society can already

be felt with the content mafia (aka. RIAA) demanding access to all data to preserve their dead business model. We will need to build technology to preserve the freedom of speech, the freedom of thought, the freedom of communication, there is no other long-term solution. Political barriers to total surveillance have a very limited half-life period.

The universal acceptance of electronic communication systems has been a tremendous help for political movements. It has become a bit more difficult and costly to maintain secrets for those in power. Unfortunately, the same problem applies to everybody else. So one thing that we can do to help societies progress along is to provide tools, knowledge and training for secure communications to every political and social movement that shares at least some of our ideals. We should not be too narrow here in choosing our friends, everyone who opposes centralistic power structures and is not geared towards totalitarism should be welcome. Maintaining the political breathing spaces becomes more important than what this space is used for.

Anonymity will become the most precious thing. Encrypting communications is nice and necessary but helps little as long as the communication partners are known. Traffic analysis is the most valuable intelligence tool around. Only by automatically looking at communications and movement patterns, the interesting individuals can be filtered out, those who justify the cost of detailed surveillance. Widespread implementation of anonymity technologies becomes seriously urgent, given the data retention laws that have been passed in the EU. We need opportunistic anonymity the same way we needed opportunistic encryption. Currently, every anonymization technology that has been deployed is instantly overwhelmed with file sharing content. We need solutions for that, preferably with systems that can stand the load, as anonymity loves company and more traffic means less probability of de-anonymization by all kinds of attack.

Closed user groups have already gained momentum in communities that have a heightened awareness and demand for privacy. The darker parts of the hacker community and a lot of the warez trading circles have gone â€œblackâ€ already. Others will follow. The technology to build real-world working closed user groups is not yet there. We have only improvised setups that work under very specific circumstances. Generic, easy to use technology to create fully encrypted closed user groups for all kinds of content with comfortable degrees of anonymity is desperately needed.

Decentralized infrastructure is the needed. The peer-to-peer networks are a good example to see what works and what not. As long as there are centralized elements they can be taken down under one pretext or another. Only true peer-to-peer systems that need as little centralized elements as possible can survive. Interestingly, tactical military networks have the same requirements. We need to borrow from them, the same way they borrow from commercial and open source technology.

Design stuff with surveillance abuse in mind is the next logical step. A lot of us are involved into designing and implementing systems that can be abused for surveillance purposes. Be it webshop systems, databases, RFID systems, communication systems, or ordinary Blog servers, we need to design things as safe as possible against later abuse of collected data or interception. Often there is considerable freedom to design within the limits of our day jobs. We need to use this freedom to build systems in a way that they collect as little data as possible, use encryption and provide anonymity as much as possible. We

need to create a culture around that. A system design needs to be viewed by our peers only as â€œgoodâ€ if it adheres to these criteria. Of course, it may be hard to sacrifice the personal power that comes with access to juicy data. But keep in mind, you will not have this job forever and whoever takes over the system is most likely not as privacy-minded as you are. Limiting the amount of data gathered on people doing everyday transactions and communication is an absolute must if you are a serious hacker. There are many good things that can be done with RFID. For instance making recycling of goods easier and more effective by storing the material composition and hints about the manufacturing process in tags attached to electronic gadgets. But to be able to harness the good potential of technologies like this, the system needs to limit or prevent the downside as much as possible, by design, not as an after-thought.

Do not compromise your friends with stupidity or ignorance will be even more essential. We are all used to the minor fuckups of encrypted mail being forwarded unencrypted, being careless about other peoples data traces or bragging with knowledge obtained in confidence. This is no longer possible. We are facing an enemy that is euphemistically called â€œGlobal Observerâ€ in research papers. This is meant literally. You can no longer rely on information or communication being â€œoverlookedâ€ or â€œhidden in the noiseâ€. Everything is on file. Forever. And it can and will be used against you. And your â€œinnocentâ€ slip-up five years back might compromise someone you like.

Keep silent and enjoy or publish immediately may become the new mantra for security researchers. Submitting security problems to the manufacturers provides the intelligence agencies with a long period in which they can and will use the problem to attack systems and implant backdoors. It is well known that backdoors are the way around encryption and that all big manufacturers have an agreement with the respective intelligence agencies of their countries to hand over valuable â€œ0 dayâ€ exploit data as soon as they get them. During the months or even years it takes them to issue a fix, the agencies can use the 0 day and do not risk exposure. If an intrusion gets detected by accident, no one will suspect foul play, as the problem will be fixed later by the manufacturer. So if you discover problems, publish at least enough information to enable people to detect an intrusion before submitting to the manufacturer.

Most important: have fun! The eavesdropping people must be laughed about as their job is silly, boring, and ethically the worst thing to earn money with, sort of blackmail and robbing grandmas on the street. We need to develop a â€œlets have fun confusing their systemsâ€-culture that plays with the inherent imperfections, loopholes, systematic problems, and interpretation errors that are inevitable with large scale surveillance. Artists are the right company for this kind of approach. We need a subculture of â€œIn your face, peeping tomâ€. Exposing surveillance in the most humiliating and degrading manner, giving people something to laugh about must be the goal. Also, this prevents us from becoming frustrated and tired. If there is no fun in beating the system, we will get tired of it and they will win. So let's be flexible, creative and funny, not angry, ideologic and stiff-necked.

———-

49 thoughts on “Welcome to the world of tomorrow”

frank Post author
7.1.2006 at 17:10

Please see also here for initial comments on the feedback we got on our talk at the 22C3 that was the base for this text.

Global Observer
11.1.2006 at 00:15

C. U.

Bilby
11.1.2006 at 22:22

A well put article Frank, imho. However, I fear it is already way too late. While I agree with the points you are making, the so-called “War on Terror” has allowed governments to place monitoring of citizens by technological means an accepted fact that is rapidly becoming “normality”. Also, as national budgets tighten, the numbers of law enforcement officers on our streets decreases. Therefore, “the majority” are quite happy to have camera’s monitor anti-social behaviour with the aim of identifying and catching perpetrators. It is the usual case of the many having to pay becuase of the stupidity of the few.

It is only older generations that can see what we are losing. The next generation and successive generations will accept these intrusions as part of their way of life, the way things are. I also believe in the not-too-distant future all citizens will have to provide samples of their DNA that will be used in creating personal ID numbered-biometric DNA cards that will then be used in conjunction with anything you do such as opening banks accounts, tax returns, government assistance right across the full spectrum of social programs, hire-purchase, obtaining credit cards, insurance, travelling, buying a car, etc.,etc. In fact, in just about any aspect of life that I can think of you will need to be able to produce your national ID DNA card. I also believe as babies are born they will have samples of their DNA taken and this sample will be added added to a database. This will finally give governments the power to monitor citizens from the cradle to the grave whenever they choose to do so. Criminality will be fought with DNA evidence becoming the prime tool in combating all crime. You will have to notify government of each and every change of your address, otherwise you will be committing a criminal offense if discovered otherwise. The list just

goes on and on. It's a world that I will not see too much of and am glad of that fact. But, it is a world that will be, make no mistake. Anonymity will not be possible.

There will be people that will fight against this new world and try to subvert or hamper the systems in various ways. But there will also be very bright people who believe 100% in the system and what it does and will do everything within their power and skills to make it uncrackable and impregnable to these subversive efforts. Of course, anyone caught in deemed subvertive actions will pay a criminal price for their actions. All-in-all a rather bleak and depressing outlook for the future.

I am really glad you wrote the article and sorry that some people cannot see what we are losing.

Regards,
Jojam

Pingback: netzpolitik.org: » Anonymer Internet-Zugang wird kriminalisiert » Aktuelle Berichterstattung rund um die politischen Themen der Informationsgesellschaft.

paris turf
30.10.2011 at 23:13

Good tip. I did it and it worked. Thanks.

Pingback: Legal Book Review – Incorporating Your Small Business | Toutes les news

Kris Manjarres
5.1.2012 at 10:30

Thanks for the post. I will definitely return. I loved as much as you will receive carried out right here. The sketch is tasteful, your authored subject matter stylish. nonetheless, you command get got an shakiness over that you wish be delivering the following. unwell unquestionably come more formerly again since exactly the same nearly a lot often inside case you shield this hike.

Voyage Dentaires
3.5.2013 at 12:03

We have not lost this war as I know?
thank you for your post